PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF:

Yen et al.

APPLICATION NO.: 10/727,332

FILED: DECEMBER 2, 2003

FOR: **DELIVERY OF LICENSE INFORMATION USING A SHORT MESSAGING PROTOCOL IN A CLOSED CONTENT DISTRIBUTION SYSTEM**

EXAMINER: Farid Homayoumehr

ART UNIT: 2439

CONFIRMATION NO: 5294

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal to the Board of Patent Appeals and Interferences from the decision of Examiner Homayounmehr mailed February 3, 2009, in which pending claims 1-17, 19-21, 25-65, 69-84, 86, 87, 89-97 stand in final rejection.

The present paper is Appellant's Appeal Brief submitted in compliance with 37 C.F.R. §41.37(c).

REAL PARTY IN INTEREST

The real party in interest is BroadOn Communications, Inc, the assignee of the entire right, title and interest in the present application.

RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any appeals or interferences which would directly affect or be directly affected by or have a bearing on the Board's decision in the present appeal.

STATUS OF CLAIMS

The application was initially filed with 90 claims. Claims 18, 22-24, 66-68, 85, 88 were canceled. Claims 91-97 are new. The final rejection of pending claims 1-17, 19-21, 25-65, 69-84, 86, 87, 89-97, as presented in Appendix A, is appealed.

STATUS OF AMENDMENTS

All amendments submitted to date have been considered and entered by the Examiner.

SUMMARY OF CLAIMED SUBJECT MATTER

What is claimed is providing a license that includes rights for content and a rule associated with a state of execution of the content for determining rights to additional content. Claim 1 includes the language:

receiving information associated with a playback device; [Pg. 13, line 19 to pg. 14, line 11; pg. 21, line 17 to pg. 18, line 5]

generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system; [Pg. 22, line 19 to pg. 23, line 11]

sending the text-based activation code to a communication device, via a transport technique not including the playback device; [Pg. 21, lines 7-15]

wherein, in operation, a user of the communication device communicates at least a portion of the text-based activation code to the playback device; [Pg. 23, lines 6-11]

further wherein, in operation, the playback device uses at least a portion of the text-based activation code to obtain rights to the content. [Pg. 23, lines 6-11]

Claim 25 includes the language:

generating a text-based activation code of a sufficiently small size that is convenient for a human to enter based on information associated with a playback device of a system; [Pg. 22, line 19 to pg. 23, line 11]

providing the text-based activation code via an SMS technique; [Pg. 21, line 7-15]

sending the text-based activation code in a text-based message to a hand-held device using an SMS technique, the text-based activation code including information from which rights information is verifiable by the system, [Pg. 21, lines 7-15]

wherein, in operation, a user of the hand-held device communicates at least a portion of the message to the playback device; [Pg. 23, lines 6-11]

putting together, at the playback device, at least an identity of the playback device and an identity of content; [Pg. 21, line 17 to pg. 22, line 5]

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate execution rights for the playback device for the content, wherein the text-based activation code is not used to authenticate the execution rights; [Pg. 21, line 17 to pg. 22, line 5]

verifying the execution rights using at least part of the text-based activation code as a cryptographic signature; [Pg. 15, lines 14-20]

launching, when the execution rights are verified, content on the playback device in accordance with the execution rights. [Pg. 13, line 19 to pg. 14, line 11]

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds for review on appeal are:

1. whether claims 1-17 and 19-21 are patentable over U.S. Patent Publication No. 2003/0120541 (Siann et al.), in view of U.S. Patent 6,859,535 (Tatebayashi et al.) under 35 U.S.C. §103(a);

2. whether claims 25-65, 69-84, 86, 87, 89-97 are patentable over Siann et al., in view of Tatebayashi et al., and further in view of Examiner Official Notice under 35 U.S.C. §103(a).

ARGUMENT

I. First Ground: Independent Claim 1

The first ground for review is whether claims 1-17 and 19-21 are patentable over Siann et al., in view of Tatebayashi et al. under 35 U.S.C. §103(a). A Final Office Action dated February 3, 2009 ("the Office Action"), included the Examiner's rationale for finally rejecting the claims.

Patent examiners carry the responsibility of making sure that the standard of patentability enunciated by the Supreme Court and by the Congress is applied in each and every case. The Supreme Court in Graham v. John Deere, 383 U.S. 1, 148 USPQ 459 (1966), stated:

> Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

The Alleged Prior Art

Siann et al.

Siann et al. apparently disclose a method and device for electronically providing electronic media content and advertising content includes a media player and electronic media content from an electronic media content provider. The media player is electronically provided with the electronic media content via a first method of transmission. The media player is also electronically provided with advertising content, from an advertising content provider, via a second method of transmission. If necessary, the electronic media content is decrypted by the media player prior to the electronic media content being provided to the user. The media player electronically determines when advertising is to be played on the media player. Additionally, according to an embodiment, when the media player is disconnected from the first method of transmission, and the media player ceases to receive electronic media content via the first

method of transmission, the media player is electronically provided with advertising content via the second method of transmission. (Abstract).

The Examiner asserts at page 3 of the Office Action that Siann et al. disclose generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system. The Examiner relies upon several paragraphs of Siann et al. and the applicants' specification. Specifically, the Examiner asserts at page 3 of the Office Action that:

> Paragraph 39 [of Siann et al.] describes access data as, for example, an authorization code which is used to ensure that the media player can decrypt the content. Therefore, access data is used to permit execution of content (content being displayed) in the player device, which is the same as description of the activation code in the applicant's specification page 15 lines 8-12. Paragraphs 97-98 clearly shows that access data is used to control access using cryptographic techniques which verify the data and allow access if the rules are satisfied. Paragraph 100 teaches configuring and providing (generating) the access data based on information specific to the certain media player. This information must be received at the device which generates the activation code so that it could be used in generation of the code.

Siann et al. state in paragraph 39: "'Access data' refers to data, for example decryption keys, that is used to ensure that a media player can decode secured electronic media content. Access data can be in the form of decryption keys, authorization codes, or the like." As an initial matter, it should be noted that there is no suggestion in Siann et al. that the access data is text-based. Nor is there any reason why Siann et al. would wish to make the access data text-based, since the access data is simply provided from one machine to another. The text-based access data issue is described in more detail later with reference to Tatebayashi et al.

Siann et al. provide a description of how to use access data (i.e., to decrypt content), and elsewhere Siann et al. provide no alternative embodiment showing that the access data is used in any other way. For example, in paragraph 80, Siann et al. state: "FIG. 1B illustrates another embodiment of the present invention that includes access data. FIG. 1B is similar to

FIG. 1A with the addition of a coordination system 160 that provides access data 164. Access data 164 is provided to the media player 120 from a coordination system 160. The coordination system 160 is the system that oversees the providing of electronic media content and advertising content to the media players and in one embodiment oversees the payment of revenue from advertising content providers to electronic media content providers. Access data 164 allows the electronic media content 110 to be secure, such that the electronic media content 110 is useable only if the proper access data has been provided to the media player 120. By using access data, secure electronic media content is decrypted."

Based upon this teaching, the Examiner makes a logical leap to allege "[t]herefore, access data is used to permit execution of content (content being displayed) in the player device, which is the same as description of the activation code in the applicant's specification page 15 lines 8-12." Page 15, lines 8-12, of the applicants' specification states: "The phrase 'activation code' describes a part of a whole license, considered necessary and sufficient to permit execution of selected specific content by the specific player device. An activation code might be an entire license, a part thereof, or a transformation thereof (such as a transformation suitable for human reading or data entry)." There is no apparent reason why Siann et al. at the time the present application was filed would provide access data that is suitable for human reading or data entry. There is also no apparent reason why Siann et al. would use access data (referred to only as a "decryption key" when actual use is described) to describe a part of a whole license or a part thereof. Thus, the Examiner's assertion that the access data of Siann et al. is "the same as description of the activation code in applicant's specification page 15 lines 8-12" is without support in the cited prior art. The applicants respectfully requested that the Examiner withdraw the assertion or provide an affidavit showing that the Examiner is able to make such an assertion without the benefit of a prior art reference, but no such affidavit was provided. When a rejection in an application is based on facts within the personal knowledge of an employee of the Office, the data shall be as specific as possible, and the reference must be supported, when called for by the applicant, by the affidavit of such employee, and such affidavit shall be subject to contradiction or explanation by the affidavits of the applicant and other persons. (See 37 CFR 1.104(d)(2)).

The Examiner asserts at page 3 of the Office Action that "Paragraphs 97 and 98 [of Siann et al.] clearly shows that access data is used to control access using cryptographic

techniques which verify the data and allow access if the rules are satisfied." It should be noted that paragraphs 97 and 98 describe nothing more than access data being used as a decryption key, and separate access rules. The applicants note that the Examiner is apparently trying to morph access data into something other than a decryption key, which is the only use Siann et al. illustrates for the access data, and, indeed, the use described in paragraph 97. Siann et al. describe using access data to decrypt content, and access rules to determine rights. These are distinct.

The Examiner asserts at page 3 of the Office Action that "Paragraph 100 teaches configuring and providing (generating) the access data based on information specific to the certain media player. This information must be received at the device which generates the activation code so that it could be used in generation of the code." However, paragraph 100 simply explains that access data and access rules can be delivered in a cryptographically secure manner, and perhaps to groups of playback devices. The Examiner's assertion that Siann et al. teach configuring and providing the access data based on information specific to the certain media player is at odds with the explicit language of Siann et al., which is:

> [0100] According to an embodiment, to provide flexibility in the use of cryptographic mechanisms for such security, access data storage device 436 contains tables of parameters which include an identification part and a cryptographic key part, such that both are used to deliver access data and access rules, and other information to the media player in a cryptographically secure manner. A further embodiment allows access rules, access data and other generalized messages to be delivered to the media player uniquely, by groups, or globally, according to how the identification parameters are defined, and how their associated key variable parts are employed. Some or all of such parameters are specific and/or confidential to a certain media player, groups of players, or other such combinations. The system is not limited to a particular cryptographic security solution, but instead, the use of media player identifications can be based upon "groupings," multi-variable key sets that can be used with such grouping identifications, and the basis for system security and trust requirements for communications over the first, second and third methods of

transmission can be supported by parametric data stored in the media player to effect cryptographic levels of security.

Contrary to the Examiner's assertion, at paragraph 100, Siann et al. say nothing about generating the access data based on information specific to the certain media player. It is not true that "This information must be received at the device which generates the activation code so that it could be used in generation of the code." The access data storage device 436 seems to generate the access data distinctly from the media player.

The Examiner takes the position that the "media player" of Siann et al. is not a "playback device," but rather is a combination of a "playback device," a "transmission/reception device," and a "device to enforce the access rules." In this way, the Examiner believes that he can argue that communications to the "transmission/reception device" are "via a transport technique not including the playback device." However, the Examiner apparently relaxes this interpretation when applying the Tatebayashi reference, as is described below with reference to Siann/Tatebayashi.

The Examiner does not attempt to assert that Siann et al. disclose a text-based activation code or a user communicates at least a portion of the activation code to the playback device (the access data is directly transmitted to the media player), and relies upon Tatebayashi et al. to make up for the deficiency.

Tatebayashi et al.

Tatebayashi et al. apparently disclose the media inherent key storing unit 220 prestores an inherent key Ki, the conversion unit 230 generates an encrypted inherent key Ji from the inherent key read from the media inherent key storing unit 220, the random number generating unit 331 generates a random number R1, the encryption unit 252 generates an encrypted random number S1, the decryption unit 333 generates a random number R'1 from the encrypted random number R1, and the mutual authentication control unit 334 compares the random number R'1 with the random number R1 and, if the random number R'1 matches the random

number R1, judges that the memory card 200 is an authorized device. If the memory card 200 and the memory card writer have successfully authenticated each other, the memory card writer encrypts a content using a decrypted inherent key. If the memory card 200 and the memory card reader have successfully authenticated each other, the memory card reader decrypts an encrypted content using the decrypted inherent key. (Abstract).

The Examiner asserts at page 4 of the Office Action that Tatebayashi et al. disclose at col. 5, line 64 to col. 6, line 10, "an embodiment where the user has to enter part of a key so the access to the content is allowed." However, Tatebayashi et al. disclose that a user can enter a password. As Tatebayashi explain, "The user key means a password that is determined by each user, is known only by the user, and is inherent in the user. Also, the user key is a combination of alphabets, numbers, and symbols." Col. 37, lines 61-65. Notably, the user key is not associated with information obtained from the playback device. It is made up by and is inherent in a user.

Siann et al. and Tatebayashi et al. Combined

As was described with reference to the cited references, Siann et al. and Tatebayashi et al. fail to disclose that which the Examiner has asserted they do, which allegedly corresponded to the elements of the claims. It follows that Siann/Tatebayashi also fails to teach each and every element of the claims.

Moreover, the combination would not work as described. Specifically, the Examiner has asserted that the playback device does not include a transmission/receiver device (allegedly the "media player" includes a "playback device," a "transmission/receiver device," and a "device to enforce the access rules," and therefore it is possible for Siann et al. to send the text-based activation code to a communication device, via a transport technique not including the playback device). If this is so, then the text-based activation code of Tatebayashi et al., which is input directly to the "device to enforce the access rules" (see col. 52, lines 52-65, which was cited by the Examiner), is never provided to the "playback device" either. Rather, the user key is entered and combined to encrypt files, and the combined key and encrypted files are provided to the playback device. The playback device provides the combined key and the encrypted files to the access device and the user enters the user key to facilitate decryption. So, according to

the Examiner's logic, the user in Siann/Tatebayashi never communicates at least a portion of the text-based activation code to the "playback device."

In any case, Tatebayashi et al. explicitly teach a user key that is a password associated with a user. The user key is not generated by a license server (or any other device), and the user key includes no data from which rights information is verifiable by the system.

The Alleged Prior Art Distinguished

Claim 1 includes the language:

receiving information associated with a playback device;

generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system;

sending the text-based activation code to a communication device, via a transport technique not including the playback device;

wherein, in operation, a user of the communication device communicates at least a portion of the text-based activation code to the playback device;

further wherein, in operation, the playback device uses at least a portion of the text-based activation code to obtain rights to the content.

As described above, Siann/Tatebayashi fail to disclose generating a text-based activation code. Siann/Tatebayashi fail to disclose an activation code that includes data from which rights information is verifiable by the system. Siann/Tatebayashi fail to disclose sending the activation code, as claimed, to a communication device, via a transport technique not including the playback device. Siann/Tatebayashi fail to disclose, in operation a user communicates at least a portion of the activation code, as claimed, to the playback device. Siann/Tatebayashi fail to disclose using at least a portion of the text-based activation code to

obtain rights to the content. For any of these reasons, claim 1 is allowable over the cited prior art, whether considered alone or in combination.

Claims 2-17, 19-21, 91-95, which depend from claim 1, are allowable at least for depending from an allowable base claim, and potentially for other reasons as well. For example, claim 12 includes the language, "at least a portion of the text-based activation code is provided to the playback device, wherein the playback device processes the portion of the text-based activation code and produces a licensing message suitable to be sent by the communication device." The Examiner asserts at page 8 of the Office Action that Siann et al. teaches this at paragraph 81. "Also, paragraph 90 describes content provider payments when users play their content or download the licensed content. This clearly implies a licensing message from user to content providers via Media Player. Note that per paragraph 95 the communication between the Media Player and Content Providers is two way." However, contrary to the Examiner's assertion, paragraph 81 says nothing about a licensing message suitable to be sent by the communication device. The Examiner says that paragraph 90 clearly implies a licensing message, but it does nothing of the sort. Paragraph 90 describes payments from advertisers; it has nothing to do with licensing messages from a user of the media player. Also, paragraph 95 refers only to "any low band mobile wireless two way communication system in the art" but says nothing about actual two-way communications. So claim 12, and claim 13, which depends from claim 12, are allowable for additional reasons.

II. Second Ground: Independent Claim 25

The second ground for review is whether claims 25-65, 69-84, 86, 87, 89-97 are patentable over Siann et al., in view of Tatebayashi et al., and further in view of Official Notice under 35 U.S.C. §103(a). A Final Office Action dated February 3, 2009 ("the Office Action"), included the Examiner's rationale for finally rejecting the claim.

For reasons similar to those described above with reference to claim 1, claim 25 is allowable over the cited references. The applicants note that although the Examiner has indicated Siann et al. disclose in paragraph 43 SMS as a possible "third method of transmission," Siann et al. disclose a list that is boilerplate in appearance, and never disclose an embodiment in which SMS is used, or would even make sense. Moreover, there is no suggestion that Siann et al. would be motivated to provide activation codes that are convenient

for humans to enter. There is also no suggestion that the text-based activation code be sent to a hand-held device, and then be communicated to the playback device by a user. The Examiner simply refers to the rejection of claim 1, which does not specifically recite a hand-held device.

Regarding "verifying the execution rights using at least part of the text-based activation codes as a cryptographic signature," the Examiner refers to Siann et al. paragraph 98, and acknowledges that "Siann does not explicitly teach use of activation codes as a cryptographic signature. However, Siann teaches using cryptographic techniques, such as a license to verify authenticity. As a cryptographic signature is a cryptographic verification technique, which is well-known and widely practiced at the time of invention, it would have been obvious to the one skill in art to use cryptographic signatures for verification. The motivation was to use a standard, commonly known and well developed technique to perform digital verification." The applicants respectfully disagree. The typical technique is to apply a hash function to data and encrypt with a private key to produce a signature for attachment to data. Digitally signed data is then separated into data, which is passed through a hash function, and the signature is decrypted using the signer's public key, and the hash of the data and the signature are supposed to match. It is not well-known to use part of a text-based activation code sent via SMS (or, more generally, a communication channel that does not include the playback device) and use it as a cryptographic signature for content on the playback device. The applicants respectfully requested that the Examiner withdraw the rejection, provide a reference that teaches "verifying the execution rights using at least part of the text-based activation codes as a cryptographic signature" as claimed, or provide an affidavit in accordance with 37 CFR 1.104(d)(2). No such affidavit has been provided.

For the reasons provided above with reference to claim 1, claim 25 is believed to be in a condition for allowance. Claim 26, which depends from claim 25, is allowable at least for depending from an allowable base claim and potentially for other reasons as well.

Claims 27, 34, 35, 36, 69 are allowable for reasons similar to those described with reference to claim 25. Claims 28-33, 96, 97; 37-65; 70-84, 86, 87, 89, 90, which respectively depend from claims 27; 36; 69, are allowable at least for depending from an allowable base

claim and potentially for other reasons as well. As indicated above, claims 91-95, which depend from claim 1, are allowable at least for depending from an allowable base claim.

III. Conclusion

In view of the foregoing remarks, Appellants submit that the pending claims are in condition for allowance and patentably define over the prior art, and urge the Board to overturn the Examiner's rejections.

Dated: August 3, 2009

Respectfully submitted,

By 

William F. Ahmann
Registration No.: 52,548
PERKINS COIE LLP
P.O. Box 1208
Seattle, Washington 98111-1208
(650) 838-4300
Attorney for Applicant

CLAIMS APPENDIX

Listing of Claims:

1. (Previously Presented) A method including steps of:

receiving information associated with a playback device;

generating a text-based activation code associated with the information obtained from the playback device, wherein the text-based activation code includes data from which rights information is verifiable by the system;

sending the text-based activation code to a communication device, via a transport technique not including the playback device;

wherein, in operation, a user of the communication device communicates at least a portion of the text-based activation code to the playback device;

further wherein, in operation, the playback device uses at least a portion of the text-based activation code to obtain rights to the content.

2. (Previously Presented) A method as in claim 1, including steps of ensuring that only authorized content is executed or presented by the playback device or a secure processor, or by both in combination or conjunction.

3. (Previously Presented) A method as in claim 1, including steps of sending the content to the playback device using a communication link not used by the steps of sending the text-based activation code.

4. (Original) A method as in claim 1, wherein the steps of enforcing are performed at least in part by the playback device or a secure processor coupled thereto.

5. (Original) A method as in claim 1, wherein the steps of enforcing are performed by mandatory security hardware or mandatory security software.

6. (Previously Presented) A method as in claim 1, wherein the steps of enforcing include steps of decrypting at least some information derivable from the text-based activation code.

7. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes using a key derived from the text-based activation code for decrypting a license or the content.

8. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes

putting together at least an identity of the playback device and an identity of the content;

applying at least part of the text-based activation code, the identity of the playback device, and the identity of the content to authenticate the execution rights for the playback device for the content.

9. (Previously Presented) A method as in claim 1, wherein the steps of enforcing includes applying a key derived from the text-based activation code as an authentication code.

10. (Previously Presented) A method as in claim 1, wherein the text-based activation code is included in an SMS.

11. (Previously Presented) A method as in claim 1, wherein at least a portion of the text-based activation code is manually entered into the playback device.

12. (Previously Presented) A method as in claim 1, wherein at least a portion of the text-based activation code is provided to the playback device, wherein the playback device processes the portion of the text-based activation code and produces a licensing message suitable to be sent by the communication device.

13. (Previously Presented) A method as in claim 12, wherein the licensing message is encrypted or cryptographically authenticated by the communication device and sent to a license server.

14. (Previously Presented) A method as in claim 1, wherein the steps of enforcing include steps of using a decryption key available to the playback device or a secure processor coupled thereto.

15. (Previously Presented) A method as in claim 1, wherein said text-based activation code is included in a first message, further comprising:

sending a second message from the communication device to a license server;

sending the first message from the license server to the communication device, the first message including human-readable characters;

manually entering those characters to an input element coupled to the playback device.

16. (Previously Presented) A method as in claim 1, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based activation code.

17. (Previously Presented) A method as in claim 1, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by a secure processor.

18. (Canceled)

19. (Previously Presented) A method as in claim 1, including steps of authenticating the rights information by the playback device or a secure processor coupled thereto.

20. (Previously Presented) A method as in claim 1, further comprising decrypting at least some information derivable from the text-based activation code.

21. (Previously Presented) A method as in claim 1, further comprising using a decryption key available to the playback device or a secure processor coupled thereto to authenticate the rights information.

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Previously Presented) A method comprising:

generating a text-based activation code of a sufficiently small size that is convenient for a human to enter based on information associated with a playback device of a system;

providing the text-based activation code via an SMS technique;

sending the text-based activation code in a text-based message to a hand-held device using an SMS technique, the text-based activation code including information from which rights information is verifiable by the system, wherein, in operation, a user of the hand-held device communicates at least a portion of the message to the playback device;

putting together, at the playback device, at least an identity of the playback device and an identity of content;

applying at least part of the message, the identity of the playback device, and the identity of the content to authenticate execution rights for the playback device for the content, wherein the text-based activation code is not used to authenticate the execution rights;

verifying the execution rights using at least part of the text-based activation code as a cryptographic signature;

launching, when the execution rights are verified, content on the playback device in accordance with the execution rights.

26. (Previously Presented) A method as in claim 25, wherein the playback device includes at least one of rights-enforcing hardware, rights-enforcing software, further including:

authenticating the rights information using the rights-enforcing hardware or rights-enforcing software;

enforcing the rights information on the system using the rights enforcing hardware or rights enforcing software, in response to the text-based activation code.

27. (Previously Presented) A method including steps of

providing a system including a secure processor and a playback device under control of the secure processor;

generating an activation code based on information associated with the playback device;

sending a text-based message including the activation code to a hand-held device using an SMS technique, the activation code including information from which rights

information is verifiable, wherein, in operation, a user of the hand-held device communicates at least a portion of the text-based message to the system;

authenticating the rights information at the secure processor in response to mandatory security software executed by the secure processor;

using the activation code as a cryptographic signature to cryptographically verify rights information;

enforcing, using the mandatory security software, the rights information on the system in response to that text-based message;

wherein the enforcing includes constructing a license using information available to the playback system, not using the activation code.

28. (Original) A method as in claim 27, including steps of sending content to the playback device using a communication link not used by the steps of sending a text-based message.

29. (Original) A method as in claim 27, wherein the steps of sending a text-based message include a transport technique not including the playback device.

30. (Original) A method as in claim 27, wherein the steps of sending a text-based message include steps of

sending a first message from a hand-held device using an SMS technique to a license server;

sending a second message from the license server to the hand-held device, the second message including human-readable characters; and

entering those characters to an input element coupled to the secure processor.

31. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of delivering content to the playback device using a second transport technique not including that used by the steps of sending a text-based message, the closed content distribution system including the mandatory security software being responsive to a private key in a public-key cryptosystem.

32. (Original) A method as in claim 27, wherein the system includes a closed content distribution system capable of ensuring that only authorized content is presented by the playback device or executed by the secure processor.

33. (Previously Presented) A method as in claim 27, wherein

the text-based message includes an authentication code; and

the system includes a secure processor capable of authenticating content coupled to the playback device in response to the activation code.

34. (Previously Presented) A method comprising

providing a system including a playback device under control of a secure processor;

generating a signature over a token including a playback device identity and content identity obtained from the playback device;

sending the signature to a hand-held device using an SMS technique, wherein, in operation, a user of the hand-held device provides the signature to the playback device identified in the token;

constructing a license using information available to the playback system, not using the signature;

authenticating the license using the signature;

enforcing, using security software at the playback device, a check against the playback device and the content identified in the token.

35. (Previously Presented) A method comprising

providing a system including a playback device under control of a secure processor;

generating an activation code based on information obtained from the playback device;

sending a text-based message including the activation code to a hand-held device using an SMS technique, the activation code including information from which rights information is verifiable by the system wherein, in operation, a user of the hand-held device provides a signature associated with the activation code to the secure processor;

constructing a license using an identity of the playback device and not using the signature;

enforcing the rights information at the secure processor using the signature and the license.

36. (Previously Presented) A method comprising:

generating an activation code based on information obtained from a playback device;

providing, in a closed content distribution system, an SMS text message that includes license information in the form of the activation code that is small enough for a human to conveniently enter, the closed content distribution system including the playback device and a secure processor, wherein the SMS message is sent via a communication link not including the playback device or secure processor, wherein, in operation, at least part of the SMS message is communicated to the playback device by a recipient of the SMS message;

constructing, at the playback device, license parameters including a device ID, a content ID, and a rights code identified by the activation code;

using at least part of the SMS text message as a signature to authenticate the constructed license parameters;

allowing content identified by the content ID to be executed or presented by the playback device or the secure processor, or by both in combination or conjunction in accordance with the constructed and authenticated license parameters, wherein the playback device or the secure processor, or both in combination or conjunction, are associated with the device ID;

ensuring that rights information associated with the rights code is enforced by the playback device or the secure processor, or by both in combination or conjunction.

37. (Original) A method as in claim 36, including steps of authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction.

38. (Original) A method as in claim 36, including steps of determining in response to the rights information whether the user is authorized to execute or present the selected content.

39. (Original) A method as in claim 36, including steps of encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

40. (Original) A method as in claim 36, including steps of receiving content at the playback device.

41. (Original) A method as in claim 36, wherein at least a portion of the content is ~~12~~ included on physical media transported to the playback device or secure processor.

42. (Original) A method as in claim 36, wherein at least a portion of the content is present at the playback device or secure processor before the steps of delivering license information.

43. (Original) A method as in claim 36, wherein the communication link includes a cellular telephone.

44. (Original) A method as in claim 36, wherein the content can be executed or interpreted by the playback device or the secure processor, or by both in combination or conjunction.

45. (Original) A method as in claim 36, wherein the content can be presented in a human-sensible form by the playback device or the secure processor, or by both in combination or conjunction.

46. (Original) A method as in claim 36, wherein the secure processor includes a computing device capable of enforcing mandatory execution of selected security software.

47. (Original) A method as in claim 36, wherein the secure processor includes a 14 computing device capable of general purpose processing.

48. (Previously Presented) A method as in claim 36, wherein the steps of providing include steps of sending a text-based message to a hand-held device using an SMS technique, the text-based message including information from which rights information is derivable.

49. (Original) A method as in claim 36, wherein the steps of ensuring include steps of decoding the license information;

generating at least a portion of the rights information in response to the steps of decoding; and

enforcing the rights information.

50. (Previously Presented) A method as in claim 36, including steps of performing a commercial transaction concurrently with communication between a license server and a user.

51. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving information at the license server sufficient to allow that license server to effect a purchase transaction by the user.

52. (Original) A method as in claim 50, wherein the steps of performing a commercial transaction include steps of receiving proof of purchase at the license server of a license by the user.

53. (Original) A method as in claim 36, including steps of performing mandatory security software by the secure processor.

54. (Original) A method as in claim 53, wherein the steps of performing mandatory security software include one or more of:

authenticating at least one of: a specific content element, a specific playback device or secure processor, a specific user;

enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

enforcing comparison of rights information with an identity of selected content available to the playback-device or the secure processor, or to both in combination or conjunction;

enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

enforcing verification of a signature by the license server.

55. (Previously Presented) A method as in claim 36, wherein the steps of providing include steps of delivering the activation code from a license server to a user; and

manually communicating the activation code from the user to the playback device or the secure processor.

56. (Previously Presented) A method as in claim 55, including steps of deriving license information from the activation code.

57. (Previously Presented) A method as in claim 55, including steps of decrypting content in response to the activation code.

58. (Previously Presented) A method as in claim 55, wherein the activation code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

59. (Previously Presented) A method as in claim 55, wherein the activation code includes a representation of at least a portion of a license message.

60. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include a human input device.

61. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include an input technique not part of the closed distribution system.

62. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include an SMS protocol.

63. (Previously Presented) A method as in claim 55, wherein the steps of communicating the activation code include a text messaging protocol.

64. (Previously Presented) A method as in claim 55, wherein the activation code includes a representation of a content decryption key.

65. (Original) A method as in claim 64, wherein the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

66. (Canceled)

67. (Canceled)

68. (Canceled)

69. (Previously Presented) A system comprising:

a closed content distribution system including a playback device and a secure processor;

a communication link not including the playback device or secure processor;

a license server capable of being coupled to the communication link;

wherein the playback device or the secure processor, or both in combination or conjunction, includes mandatory security software that is capable of verifying rights information associated with a license from a text-based activation code received on the communication link, wherein the text-based activation code is generated based on information obtained from the playback device, wherein at least a portion of the text-based activation code is communicated from a user to the playback device or secure processor, wherein license parameters of the license do not include the text-based activation code, and wherein the text-based activation code includes a signature used to cryptographically verify the license.

70. (Original) Apparatus as in claim 69, wherein at least a portion of the content is included on physical media transported to the playback device or secure processor.

71. (Original) Apparatus as in claim 69, wherein the communication link includes a cellular telephone.

72. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the license information.

73. (Original) Apparatus as in claim 69, wherein the mandatory security software includes instructions determining in response to the rights information whether the user is authorized to execute or present the selected content.

74. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions of

encoding the license information using a digital signature, secure hash, or shared secret; and

authenticating the license information by the playback device or the secure processor, or by both in combination or conjunction, in response to the digital signature, secure hash, or shared secret.

75. (Original) Apparatus as in claim 69, wherein

the mandatory security software includes instructions ensuring that only authorized content is executed or presented by playback device or the secure processor, or both in combination or conjunction; and

rights information derivable from the license information is enforced by the playback device or the secure processor, or by both in combination or conjunction.

76. (Original) Apparatus as in claim 69, wherein the mandatory security software includes one or more of:

instructions authenticating at least one of: a specific content element, a specific playback device or secure processor, and a specific user;

instructions enforcing comparison of an identity associated with the playback device with a tamper-proof identity available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing comparison of rights information with an identity of selected content available to the playback device or the secure processor, or to both in combination or conjunction;

instructions enforcing computation of the secret key (using its private key and server public key) and decryption of the identities; and

instructions enforcing verification of a signature by the license server.

77. (Original) Apparatus as in claim 69, wherein the secure processor includes a computing device capable of general purpose processing.

78. (Original) Apparatus as in claim 69, including a code delivered from a license server to a user, the code being communicated from the user to the playback device or the secure processor.

79. (Original) Apparatus as in claim 78, including a content decryption key embedded in the code.

80. (Original) Apparatus as in claim 78, including a human input device coupled to the playback device or the secure processor.

81. (Original) Apparatus as in claim 78, including license information embedded in the code.

82. (Original) Apparatus as in claim 78, including an SMS protocol message.

83. (Original) Apparatus as in claim 78, including a text messaging protocol message.

84. (Original) Apparatus as in claim 78, wherein the code includes a human-readable alphabetic, alphanumeric, numeric, or other character string.

85. (Canceled)

86. (Original) Apparatus as in claim 78, wherein the code includes a representation of a content decryption key.

87. (Original) Apparatus as in claim 86, wherein

the closed distribution system includes a public-key cryptosystem; and

the content decryption key includes a decryption key privately associated with the content, encrypted by an encryption key publicly associated with a specific playback device.

88. (Canceled)

89. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific user.

90. (Previously Presented) Apparatus as in claim 69, wherein the mandatory security software includes instructions authenticating the code, the instructions including one or more of:

instructions determining if the code is digitally signed by a license server; and

instructions determining if the code is encrypted by a key known commonly to both the license server and the specific playback device or secure processor, or both in combination or conjunction.

91. (Previously Presented) A method as in claim 1, further comprising:

constructing parameters of execution rights for the hand-held device or the content;

providing a system including a playback device;

sending to the playback device, via a transport technique not including the playback device, a text-based message associated with an SMS technique, wherein the text-based message is derivable by the system;

enforcing, using mandatory security hardware or mandatory security software, the rights information on the system in response to the text-based message, said enforcing including:

constructing parameters of execution rights for the playback device;

using at least part of the text-based message as a signature to authenticate the execution rights.

92. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes using at least part of the text-based activation code as a cryptographic signature generated using a private key of a public key cryptographic key pair.

93. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes computing a cryptographic signature using a computed shared secret key to construct a message authentication code (MAC).

94. (Previously Presented) A method as in claim 1, wherein the cryptographically verifying includes decrypting the text-based activation code using a computed shared secret key and matching the decrypted text-based activation code against the license parameters.

95. (Previously Presented) A method as in claim 1, wherein one or more of the license parameters are selected from the group consisting of: a device identity, a content identity, and a rights code.

96. (Previously Presented) A method as in claim 27, further comprising using at least part of the activation code as a cryptographic signature generated using a private key of a public key cryptographic key pair.

97. (Previously Presented) A method as in claim 27, further comprising:

using at least part of the activation code as an encrypted message from a license server;

decrypting said encrypted message using a shared secret key computed by the playback device;

verifying that the decrypted message verifies against said constructed license.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None